

# Cisco Catalyst SD-WANルータのDoS脆弱性



アドバイザリーID : cisco-sa-sdwan-utd-dos-hDATqxs

[CVE-2024-20455](#)

初公開日 : 2024-09-25 16:00

バージョン 1.0 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwi07137](#)

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

## 概要

Cisco IOS XEソフトウェアのUnified Threat Defense(UTD)コンポーネントにコントローラモードで送信されるトラフィックを分類するプロセスの脆弱性により、認証されていないリモートの攻撃者が該当デバイスにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、SD-WAN IPSecトンネルから出力される特定のパケットに対するUTDの処理が不適切なことに起因します。攻撃者は、該当デバイスに設定されているSD-WAN IPsecトンネルを介して巧妙に細工されたトラフィックを送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS状態が発生する可能性があります。

注:Generic Routing Encapsulation ( GRE ; 総称ルーティングカプセル化 ) が設定されたSD-WANトンネルは、この脆弱性の影響を受けません。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-utd-dos-hDATqxs>

このアドバイザリーは、Cisco IOSソフトウェアおよびIOS XEソフトウェアのセキュリティアドバイザリーバンドル公開の2024年9月リリースの一部です。アドバイザリーとリンクの一覧については、『[Cisco Event Response: September 2024 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication](#)』を参照してください。

## 該当製品

## 脆弱性のある製品

この脆弱性は、脆弱性のあるCisco IOS XEソフトウェアリリースをコントローラモードで実行し、UTDをインストールして有効にし、SD-WANトンネルがIPSecを使用するように設定されている次のシスコ製品に影響を与えます。

- 1000 シリーズ サービス統合型ルータ (ISR)
- Catalyst 8000v エッジソフトウェア
- Catalyst 8200 シリーズ エッジプラットフォーム
- Catalyst 8300 シリーズ エッジプラットフォーム
- Catalyst 8500L エッジプラットフォーム
- Catalyst IR8300 高耐久性シリーズ ルータ

注：UTDはデフォルトではこれらのデバイスにインストールされていません。UTDファイルがインストールされていない場合、そのデバイスは脆弱ではありません。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

## Cisco IOS XEソフトウェアがコントローラモードであるかどうかを確認する

デバイスがコントローラモードか自律モードかを判断するには、`show platform software device-mode` コマンドを使用します。出力に「Device Operating-mode:Controller-Managed」が含まれている場合は、デバイスがコントローラモードになっています（次の例を参照）。

```
<#root>
```

```
Router#
```

```
show platform software device-mode
```

```
Device Operating-mode:
```

```
Controller-Managed
```

```
Device-mode bootup status:
```

```
5/24 23:07:35 System is green
```

```
Router#
```

## UTD が有効かどうかを確認する方法

デバイスでUTDが有効になっているかどうかを確認するには、`show utd engine standard status` コマンドを使用します。出力のRunningの下にYesと表示されている場合は、次の例に示

すように、UTDが有効になっています。出力されない場合、デバイスは影響を受けません。詳細については、「[CLIを使用したSD-WANでのUTDエンジンのインストールとアンインストール](#)」ガイドを参照してください。

```
<#root>

Router#

show utd engine standard status

Engine version      : 1.0.19_SV2.9.16.1_XE17.3
Profile             : Cloud-Low
System memory       :
                    Usage  : 6.00 %
                    Status : Green
Number of engines   : 1
```

```
<#root>

Engine

Running

      Health      Reason
=====
Engine(#1):

Yes

      Green      None
=====
.
.
.
```

## SD-WANトンネルがIPSecを使用するように設定されているかどうかを確認する

SD-WANトンネルがIPSecを使用するように設定されているかどうかを確認するには、`show sdwan bfd sessions | include ipsec`コマンドを使用します。出力がある場合、デバイスにはIPsecを使用して設定されたSD-WANトンネルがあります。出力されない場合、デバイスは影響を受けません。次の例は、SD-WANトンネルがIPsecで設定されているデバイスでの出力結果を示しています。

```
<#root>

Router#

show sdwan bfd sessions | include ipsec
```

```
172.16.255.13 300 up mp1s mp1s 192.168.0.1 192.168.1.1 12366
```

```
ipsec
```

```
7 1000 0:00:02:50 0
```

```
Router#
```

## 脆弱性を含んでいないことが確認された製品

このアドバイザリの[脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。](#)

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Catalyst SD-WANコントローラソフトウェア (旧称: SD-WAN vSmartコントローラソフトウェア)
- Catalyst SD-WAN Manager Software (旧称SD-WAN vManage Software)
- Catalyst SD-WAN Validatorソフトウェア (旧称SD-WAN vBond Orchestrator Software)
- Catalyst SD-WAN vEdge Cloudルータ
- Catalyst SD-WAN vEdgeシリーズルータ
- IOS ソフトウェア
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

## 回避策

この脆弱性に対処する回避策はありません。ただし、UTD機能が不要な環境では、UTD機能を削除または無効にすることで、攻撃ベクトルを封じ込めることができます。詳細については、「[CLIを使用したSD-WANでのUTDエンジンのインストールとアンインストール](#)」ガイドを参照してください。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

## 修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェアバージョンとフィーチャセットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

<https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンスアップグレードです。無償のセキュリティソフトウェアアップデートによって、お客様に新しいソフトウェアライセンス、追加ソフトウェアフィーチャセット、またはメジャーリビジョンアップグレードに対する権限が付与されることはありません。

Cisco.com の [シスコサポート & ダウンロードページ](#)には、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス ( My Devices ) ] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

[ソフトウェアのアップグレード](#)を検討する際には、シスコセキュリティアドバイザリページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレードソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center ( TAC ) もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

## サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC ( [https://www.cisco.com/c/ja\\_jp/support/web/tsd-cisco-worldwide-contacts.html](https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html) ) に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

## Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコセキュリティアドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース ( 「First Fixed」 ) を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイ

ザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「[Cisco Software Checker](#)」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、[セキュリティ影響評価 \(SIR\)](#) が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（15.9(3)M2、17.3.3 など）を入力します。
3. [チェック (Check)] をクリックします。

2		Critical,High,Medium
このアドバイザのみ		
Enter release number	Check	

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

## 出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-utd-dos-hDATqxs>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2024年9月25日

## 利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したり

する権利を有します。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。